无线传感器网络数据分发中节点克隆攻击检测方案

张　倩，陈宏滨

（桂林电子科技大学 信息与通信学院，广西 桂林 541004）

摘　要：在无线传感器网络（WSNs）中，数据分发是一种重要的传输方式，需要满足以下要求：可靠性，节能和可扩展性。然而，现有的研究工作很少关注数据分发中所存在的攻击，导致数据分发的可靠性大打折扣。为了检测出 WSNs 数据分发中的节点克隆攻击，保证数据分发的高可靠性，提出了基于单轮零知识证明的节点克隆攻击检测方案。本方案通过构建析取-叠加码生成专属于各个节点的数字指纹，在单轮零知识证明方案中对节点的数字指纹进行验证，可以检测出没有正确数字指纹的克隆节点。仿真表明使用提出的检测方案，可以保证 WSNs 在数据分发过程中的高可靠性。

关键词：数据分发；节点克隆攻击；析取-叠加码；零知识证明；可靠性

中图分类号：TN915.9　　　　文献标志码：A　　　　文章编号：

A node cloning attack detection scheme for WSNs data dissemination

ZHANG Qian, CHEN Hongbin

（School of Information and Communication, Guilin University of Electronic Technology, Guilin 541004, China）

Abstract:In wireless sensor networks (WSNs), data dissemination is an essential transmission mode, which needs to meet three requirements: reliability, energy saving and scalability. Existing research pays little attention to the attacks in data dissemination, resulting in a significant loss of the reliability of data dissemination. In order to detect node clone attacks in WSNs data dissemination and ensure high reliability of data dissemination, a node clone attack detection scheme based on single round zero knowledge proof is proposed. In this scheme, the digital fingerprint of each node is generated by constructing superimposed disjunct code, and the cloned node without correct digital fingerprint can be detected by verifying the digital fingerprint of the node in the single round zero-knowledge proof scheme. Simulation results show that the proposed scheme can ensure the high reliability of WSNs in the data dissemination process.

Key words: data dissemination; node clone attack; superimposed disjunct code; zero knowledge proof; reliability

在无线传感器网络（wireless sensor networks，简称 WSNs）中，最常见的工作是基站或汇聚节点（Sink 节点）从感知区域中散布的节点中收集感知数据[1]。相对于数据收集这种多对一的数据传输模式，一对多的数据传输也是 WSNs 工作中关键的一环[2]。这种数据传输形式被称作数据分发。基站或 Sink 节点在网络更新时向传感器节点发送配置参数来保持网络的一致，或者发送命令、警告等消息完成对传感器节点的控制，这类消息的传输都属于数据分发[3]。数据分发中一个重要的指标是可靠性，即 WSNs 中所有节点都应该接收到分发的数据，以此来维护网络的统一性。在数据分发过程中，如果出现节点被捕获的情况，将会严重降低数据分发的可靠性。因此在研究数据分发协议时考虑到节点捕获攻击是非常有意义的工作。

WSNs 中的数据分发要满足以下要求：可靠性、节能和可扩展性[4]。典型的数据分发方法可以分为两大类：1）基于结构的分发方案；2）无结构分发方案。基于结构的数据分发方案有：CORD[5]、CoCo[6]、CDS[7]等。在基于结构的分发方案中，利用网络结构信息（如位置和拓扑）可以构建一个高效数据分发的专用结构[8]。因此基于结构的数据分发方案满足可靠性和节能的要求，但是可扩展性较差。在无结构数据分发方案中，没有使用网络结构信息，也没有形成用于数据分发的专用结构，可扩展性很好。对于无结构分发方案，根据是否使用协商机制将其分为：1）非协商方案（如泛洪[9]、Gossip[10]、Trickle[11]等）；2）基于协商的方案（如 SPIN[12]、MOAP[13]、Deluge[14]等）。在没有控制信息的非协商方案中，数据分发过程相对较快，但难以提供高可靠性，而且非协商方案可能会导致广播风暴问题。基于协商的方案旨在控制冗余传输，保证高可靠性的要求[15]。但是采用的控制信息也给数据分发带来了额外的通信开销和时间开销，相对非协商方案，基于协商的方案节能性较差。

节点克隆攻击是 WSNs 数据分发中破坏性极大的一种攻击形式：攻击者通过捕获合法节点从而获取关于网络的敏感信息，进而把这些信息复制到克隆节点上，并重新部署克隆节点到网络中[16]。这样克隆节点可以很容易地以合法节点的身份参与到

收稿日期：2022-04-24

基金项目：国家自然科学基金（62061009）

通信作者：陈宏滨（1981-），男，教授，博士，研究方向为传感器网络。E-mail：chbscut@guet.edu.cn

WSNs 的数据分发和其它工作中，从而能够发起破坏性更广的内部攻击。本文针对节点克隆攻击的检测方案展开了研究，下面将详细介绍现有的节点克隆攻击的检测方案。

节点克隆攻击的检测方案中常用的第一类技术是比较相邻节点所拥有的信息：每个节点将自己的存储的信息与所有相邻节点的信息进行比较，通过判断存储的信息是否存在不一致来检测节点克隆攻击[17]。文献[18]提出了一种用于低功耗无线个人区域网络 IPv6（6LoWPAN）的克隆节点攻击检测协议。在该协议中，使用 6LoWPAN 映射函数给所有节点分配一个身份标识（identity，简称 ID）和秩信息，用父节点所使用的映射器特性可以识别节点 ID 和秩信息之间的异常。但是，当攻击者捕获父节点进行克隆时，将会导致检测方案失效的情况。文献[19]提出了一种用于物联网的克隆节点攻击检测方案。该方案利用基于指纹的零知识证明机制对传感器设备进行两级认证。基站为每个节点计算出指纹并发送给节点所在集群的簇头节点，通过比较每个设备的指纹与基站存储的信息来进行克隆节点的检测。在需要同时验证大量传感器节点的指纹，基站的计算开销会非常大。此外，由于该方案只适用于静态网络中，增加了簇头节点和基站之间的通信开销。

节点克隆攻击的检测方案中常用的第二种技术是使用证人发现技术：使用证人节点在通信中发现克隆节点的存在，通过合理地改变证人节点的选择方式来达到检测方案的高效性[20]。文献[21]提出了四种检测克隆攻击的方法，分别是节点到网络广播、确定性组播、随机组播和线选组播。节点到网络广播方案将位置信息泛洪到整个网络，相当于把所有节点都选择为证人节点，可以检测出身份冲突。确定性组播选择特定的一部分节点作为证人节点来降低通信成本。随机组播方案提出了将节点位置信息分发给随机选择的证人节点，可以避免攻击者获取固定证人节点的信息攻击证人节点，并且利用生日悖论[22]来检测被复制的节点。最后提出的线选组播方案利用网络拓扑结构来检测被复制的节点，使克隆攻击在证人节点连接成路径的交叉点被检测。其缺点在于检测性能受到证人节点间路径交叉点数量和分布的限制。

本文提出的检测方案属于第一种技术，通过比较原节点与克隆节点拥有的信息得出检测结果。创新点在于检测方案中应用了基于椭圆曲线离散对数的单轮零知识证明方案，相比多轮零知识证明方案，单轮零知识证明方案最大程度地减少了通信量，从而极大地减少了通信能耗。

1 系统模型

1.1 传感器网络模型

如图 1 所示，本文考虑静态的 WSNs，在网络中部署有一个 Sink 节点和大量普通节点。其中 Sink 节点放置在监测区域的中间位置，间歇性地经多跳传输向 WSNs 中的普通节点分发数据或者收集数据。Sink 节点作为 WSNs 和互联网的网关，从而实现对整个 WSNs 的管理。相对普通传感器来说，Sink 节点的能量、内存等都可以被认为是无限的。普通节点负责感知监测区域相关信息、处理感知数据并传输数据。

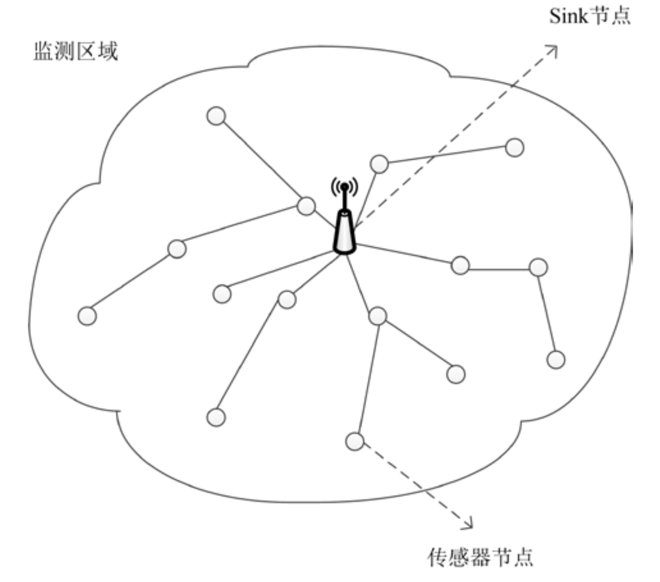


图 1 传感器网络模型

1.2 数据分发模型

本文选用基于协商的路由方案（sensor protocol for information via negotiation，简称 SPIN）作为数据分发的路由，这是一种无结构、平面型路由方案，如图 2 所示。节点间通过广播 ADV 消息告知邻居将要分发的数据，需要数据的邻居回复 REQ 消息，已经拥有分发数据的节点发送 DATA 消息给没有分发数据的节点。这种路由方案减少了分发过程中冗余数据包的传输。ADV 消息和 REQ 消息是很小的数据包，所消耗的能量资源少，但是却能保证数据分发的可靠性。采用 ADV 和 REQ 消息的传输建立的连接使得数据分发满足可靠性的要求，同时也满足可扩展性。

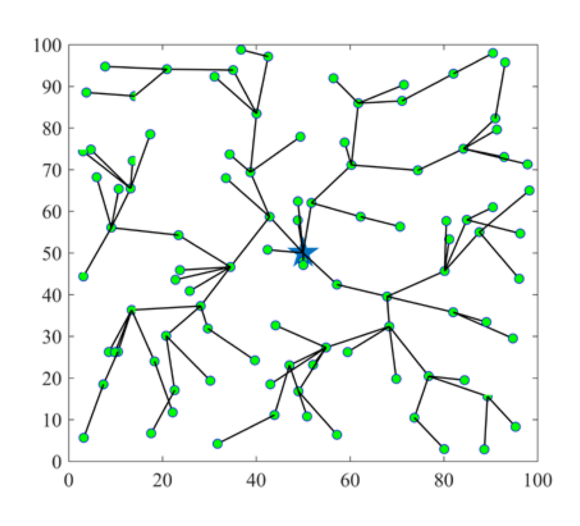


图 2 SPIN 数据分发模型

1.3 节点克隆攻击检测模型

WSNs 能得到广泛应用的一个原因是应用的都是低成本的微型传感器。因此，网络中所有的传感器节点都没有安装防篡改硬件，当一个节点遭遇到捕获攻击后，其内存中的重要信息将会被攻击者所获得。攻击者可能部署多个具有相同身份标识 ID 的节点到网络中，以便它们可以互相配合躲过检测。和大多数研究中应用的模型一样，克隆节点无法在没有基站或 Sink 节点的同意的情况下创建新的 ID，因此本文假设克隆节点只能使用原节点 ID 参与网络。

2 算法描述

为了应对数据分发中的节点克隆攻击，本文提出了单轮零知识证明的检测方案（single round zero knowledge proof，简称 SR-ZKP），该算法使用节点部署位置信息和由 Sink 节点配备给每个节点的身份证明码构建析取-分离码，可以生成专属于各个合法节点的数字指纹，继而使用数字指纹作为合法节点与克隆节点的区分依据，证明方式使用基于椭圆曲线离散对数的单轮零知识证明方案。应用到的理论知识见下文。

2.1 理论基础

2.1.1 析取-叠加码

叠加码被广泛地研究和应用于各个领域，如多址通信、密码学、模式匹配、电路复杂性等许多计算机科学领域。在密码学中的应用有复杂度低，难以破解的优点。首先介绍叠加码的基本定义和性质。

设 $\boldsymbol{X}$ 是一个 $M\times N$ 的二进制矩阵，其中 $\boldsymbol{X}_{i,j}$ 是第 i 行第 j 列的元素。在本文中，考虑一个矩阵 $\boldsymbol{X}$ 具有恒定的列权 ω 和恒定的行权 λ，即满足式(1)、(2)。

$$\sum_{i=1}^{M}\boldsymbol{X}_{i,j}=\omega \tag{1}$$

$$\sum_{i=1}^{M}\boldsymbol{X}_{i,j}=\lambda \tag{2}$$

其中，$1\le i\le M$，$1\le j\le N$。二进制矩阵 $\boldsymbol{X}$ 可以用来定义一个二进制代码，其中每列 $\boldsymbol{X}_j=(\boldsymbol{X}_{1,j},\boldsymbol{X}_{2,j},\ldots,\boldsymbol{X}_{M,j})^{\mathrm{T}}$ 对应一个码字。

对于矩阵 $\boldsymbol{X}$，有以下定义：

定义 1 覆盖。给定 2 个二进制码字 $\boldsymbol{y}=\left(y_1,y_2,\ldots,y_M\right)^{\mathrm{T}}$，$\boldsymbol{z}=\left(z_1,z_2,\ldots,z_M\right)^{\mathrm{T}}$，如果 $\boldsymbol{y}$ 和 $\boldsymbol{z}$ 的布尔和(即逻辑或操作)等于 $\boldsymbol{y}$，那么说 $\boldsymbol{y}$ 覆盖 $\boldsymbol{z}$，记做 $\boldsymbol{y}\vee\boldsymbol{z}=\boldsymbol{y}$。

定义 2 (s, L, M)叠加码。如果一个 $M\times N$ 二进制矩阵 $\boldsymbol{X}$ 的任意 s 个列的布尔和能够覆盖 $\boldsymbol{X}$ 的这 s 个列以外的最多 $L-1$ 个列，那么就说这是一个定义了长度为 M,大小为 N、强度为 $s(1<s<M)$和列表大小为 $l(l\le L-1$，并且$1\le L\le M-s)$ 的叠加码，记做(s, l, M)叠加码，大小为 N。

定义 3 析取性质的定义。如果 $\boldsymbol{X}$ 中任意 s 列的布尔和不能覆盖该 s 列集合以外的任何列时，称 $\boldsymbol{X}$ 为 s-析取码。

根据上述定义，$(s, 1, N)$叠加码也是 s-析取码，记做析取-叠加码。式(3)中的 $\boldsymbol{X}$ 是(3, 1, 13)析取-叠加码。根据析取-叠加码的析取特性，有以下性质：

给定一个$(s, 1, N)$析取-叠加码 $\boldsymbol{X}$，对于 $\boldsymbol{X}$ 的任意 s 个列的子集，至少存在一个行的所有元素都是 0。

$$\boldsymbol{X}=\begin{bmatrix}1&0&0&0&1&0&0&0&0&0&1&0&1\\1&1&0&0&0&1&0&0&0&0&0&1&0\\0&1&1&0&0&0&1&0&0&0&0&0&1\\1&0&1&1&0&0&0&1&0&0&0&0&0\\0&1&0&1&1&0&0&0&1&0&0&0&0\\0&0&1&0&1&1&0&0&0&1&0&0&0\\0&0&0&1&0&1&1&0&0&0&1&0&0\\0&0&0&0&1&0&1&1&0&0&0&1&0\\0&0&0&0&0&1&0&1&1&0&0&0&1\\1&0&0&0&0&0&1&0&1&1&0&0&0\\0&1&0&0&0&0&0&1&0&1&1&0&0\\0&0&1&0&0&0&0&0&1&0&1&1&0\\0&0&0&1&0&0&0&0&0&1&0&1&1\end{bmatrix} \tag{3}$$

2.1.2 零知识证明

零知识证明是使一方（称为证明方，记为 P）在在不泄露任何有用信息的情况下，向另一方（称为验证方，记为 V）证明自己了解某些知识。这种方式避免了因第三方的窃听而获取到知识的可能，保护了知识的完整性和保密性。这一特性适用于在开放的无线信道中验证节点的秘密信息。零知识证明方案的步骤如下：

步骤 1　P 向 V 发送与证明的知识相关的承诺信息（Commit），V 可以由此判断后续证明中 P 是否违背了该承诺信息。

步骤 2　V 在收到承诺信息后，在问题集合中随机挑选一个问题发送给 P。其中问题集合是指只可以用秘密知识解决的问题的合集。

步骤 3　P 利用自己拥有的秘密知识解决该问题，并发送给 V 做验证。

步骤 4　V 根据验证信息得出对 P 身份的判别。

由于步骤二中问题挑选的随机性，零知识方案需要多次重复这四个步骤才能保证正确性。而基于椭圆曲线的单轮零知识方案只需要进行一轮就可以达到对正确性的要求，极大地减少了证明过程中的通信成本[23]。

2.2 数字指纹生成

这一阶段使用环境信息和唯一的身份证明码构建析取-叠加码，然后生成节点的数字指纹 D_{ID}。将数字指纹 D_{ID} 用在数据分发过程中，可以检测出克隆节点。与一般的公钥协议对比，这种构建析取-叠加码进行加密的算法计算量更小，只需要进行简单的二进制操作。

一些方案将节点部署位置的邻域信息数字化为二进制代码串，把其填入矩阵的第一行，然后用循环右移的操作填充下面的行，直到矩阵各列的权值相等时停止，但是大部分传感器网络会部署较多的节点数，导致有冗余节点的存在，这样构造矩阵可能会造成具有相同邻域信息的冗余节点和邻居计算出相同的析取-叠加码，从而产成冲突。

因此，本方案使用代表邻域信息的二进制代码串作为矩阵的一部分。设置汇聚节点分配给各个节点唯一的身份证明码（也表示为二进制代码串），然后填充到当前部分矩阵的最后一列，这时还需要继续在最后一列加上身份证明码的反码串，如此来满足矩阵具有恒定权值的性质。按照这种方式到了唯一的矩阵，不仅包含了节点部署环境的特点，而且有象征节点唯一身份的数值串，并且这个数值串只被 Sink 节点和单个节点知道。

然后利用析取-叠加码的特性来构造指纹。计算指纹的方法已在现有的工作中有过介绍，计算过程如图 3 所示。

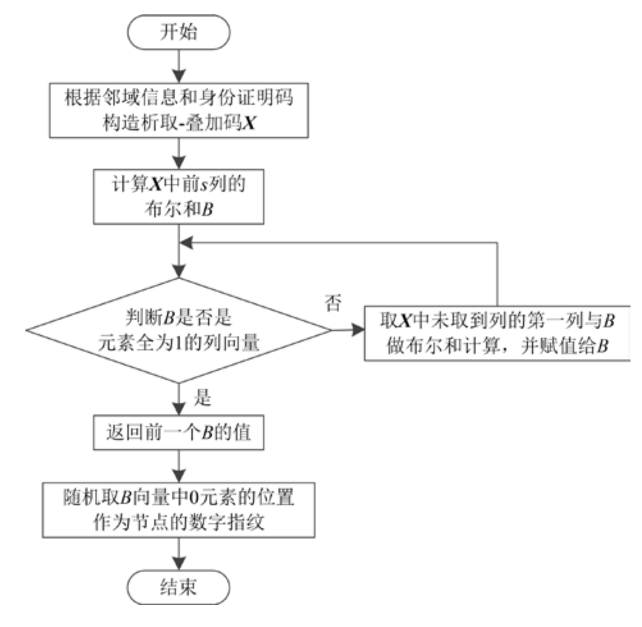


图 3 用析取-叠加码求数字指纹的过程

2.3 单轮零知识证明检测

这一阶段使用基于椭圆离散对数的单轮零知识方案来进行克隆节点的检测，可以做到在检测节点身份的同时不直接暴露节点的身份凭证。

首先描述椭圆曲线离散对数问题：给定一个有限域 $\boldsymbol{F}_p$ 和 $\boldsymbol{F}_p$ 上的一条椭圆曲线 $\boldsymbol{E}$，那么对于椭圆曲线 $\boldsymbol{E}$ 上的一个基点 G，有以下运算：

$$m \cdot G = M \left(\bmod p\right) \tag{4}$$

在知道 G、M 和椭圆曲线质数 p（p 通常选择为一个很大的素数）的前提下，求解 m 的问题即为椭圆曲线离散对数问题。基于椭圆离散对数的单轮零知识方案就是在证明方与验证方双方共享 G、M、p 的情况下，证明方 P 向验证方 V 证明他知道一个椭圆曲线上离散对数问题的解 m。椭圆曲线离散对数问题的求解需要指数时间，不知道秘密知识的证明方很难通过验证方的验证，因此在应用该问题的检测方案中克隆节点几乎不会通过检测。

在网络初始化阶段，各节点生成承诺消息 Commit，并与数字指纹打包交换给一跳邻居节点，邻居节点存储消息在内存中。承诺消息的形式为 Commit={G, M}，其中 G 是节点在椭圆曲线上随机选取的基点，p 为使用的椭圆曲线的大质数，M 由式(5)计算得来：

$$D_{\mathrm{ID}} \cdot G = M \left(\bmod p \right) \tag{5}$$

在零知识证明中，数据分发过程中的上游节点（也包括 Sink 节点）担任验证方 *V*，下游节点担任证明方 *P*。经过承诺信息的交换，这时 *P*、*V* 双方已经共享了 *p*、*G*、*M*。

在数据分发过程中，由 *V* 对下游节点发起验证：

V 使用生成承诺消息中选择的 *G*、随机选取的 *r*（$r \in \mathbf{F}_p$），用这些来计算 *B*（其中“·”指在椭圆曲线上的乘法运算），并将其发送给 *P*：

$$B = r \cdot G \left(\bmod p \right) \tag{6}$$

P 在收到验证消息后，使用只有合法节点拥有的 D_{ID}，生成 *K* 并发送给 *V*：

$$K = D_{\mathrm{ID}} \cdot B \tag{7}$$

V 接收 *K* 后，使用式(8)中的公式检查条件：

$$N_{\mathrm{flag}} = K - r \cdot M \tag{8}$$

如果式(6)得到的 N_{flag} 为 0，*V* 接收 *P* 的证明，判断 *P* 是安全可信的；如果 N_{flag} 不为 0，就判断 *P* 为克隆节点，并将检测结果传播到整个网络中，使克隆节点与 WSNs 隔离，消除克隆节点继续发动内部攻击的可能。

2.4 分析

2.4.1 安全分析

首先对零知识证明方案的完全性、正确性和零知识性进行分析。

1）完全性：由方案可以很容易地看出，如果证明方确实知道 D_{ID} 并且遵守方案指令完成方案，那么验证方总是能接受证明方的证明，即方案满足完全性。

2）正确性：假设克隆节点不知道 D_{ID}，试图欺骗上游的验证方。那就说明克隆节点要猜测椭圆曲线域上 D_{ID} 的值，而猜测正确的概率仅为 1/*p*，是一个很小的值。因此也满足正确性。

3）零知识性：在证明过程中，*V* 只能获取到关于 *P* 是否拥有秘密 D_{ID} 的内容，不会获取其它额外知识，满足零知识性。

接下来分析本方案是否能抵御最常见的中间人攻击和重放攻击：

1）中间人攻击：这是无线网络中最常见的一种攻击，攻击者把自己伪装为通信双方之间的中间构件：即在参与通信的合法发送方面前扮演接收方的身份，在参与通信的合法接收方面前扮演发送方的身份，从而控制通信。在本文提出的检测方案中，如果攻击者试图与 WSNs 中节点建立独立的连接，将会由于没有合法节点的数字指纹而无法伪装成功。在本文的方案中，节点的数字指纹具有零知识性。非法的攻击者无法知道合法节点的数字指纹。即使攻击者以极小的概率试出指纹，它还是无法通过零知识证明，因为零知识证明的每一次都会生成新的随机挑战问题。

2）重放攻击：在这种攻击中，攻击者试图重放先前的通信来消耗网络的有限资源，并向验证方验证自己。但是，由于验证方将为每次通信发送不同的挑战值，重放之前的通信将无法通过验证方的认证。

2.4.2 复杂度分析

在使用析取-重叠码计算数字指纹时，只用到简单的二进制运算。

在零知识证明中，*P* 进行椭圆曲线上的一次乘法运算，*V* 进行椭圆曲线上的两次乘法次运算和一次判断。在每轮数据分发中，每个节点都作为证明方参与一次验证；与之对应，其在分发路径中的上游节点作为验证方参与一次验证。因此在 *N* 个节点的 WSNs 中，一共要进行 *N* 次零知识证明来判断节点是不是攻击者重部署的克隆节点。完成一次零知识证明需要进行 3 次椭圆曲线上的乘法运算，整个运算过程的计算复杂度为 $\boldsymbol{O}(N)$。

对攻击者来说，求解椭圆曲线上离散对数的时间复杂度是 $\mathrm{Exp}\left(\boldsymbol{O}\left(\log \boldsymbol{p}\right)\right)$[24]，需要指数时间来求解，因此本方案具有很高的安全性。

2.4.3 可扩展性分析

本方案在 SPIN 数据分发的基础上进行克隆节点的检测，属于无结构方案。由上文分析可知，无结构方案不依赖于网络拓扑结构，具有良好的可扩展性。具体体现为随着网络规模增加，本协议的完成时间与能耗会缓慢增加。

3 仿真结果

3.1 实验仿真设置

本实验设置一个边长为 100 m 的正方形区域作为监测区域，把 Sink 节点放置在检测区域中心，采用随机的方式部署节点。为了显示节点克隆攻击对数据分发的影响，本文分别进行了无克隆攻击和克隆节点数为 5、10 时对 SPIN 分发协议影响的实验。将本文中提出的基于单轮零知识证明的节点克隆攻击检测方案（SR-ZKP）应用到 SPIN 方案中（简记为 ZKP-SPIN），即在数据分发的三条消息中加入零知识证明的三个有关于节点数字指纹的数据内容，与其它场景一同参与仿真比较。随机生成了 20 个 WSNs，在每个 WSNs 进行 400 轮数据分发，将其中每个网络性能指标的平均值展示在下面的仿真结果图中。实验中用到的参数及取值如表 1 所示。

表 1 仿真实验参数设置

参数	数值
监测区域（长×宽）	100 m×100 m
ADV 消息大小	100 bit
REQ 消息大小	100 bit
DATA 消息大小	30~35 kbit
init_num	100
clone_num	5、10
r	20 m
E_0	1 J
E_{elec}	50 nJ/bit
ε_{fs}	12 pJ/(bit • m^{-2})
ε_{amp}	0.0012 pJ/(bit • m^{-2})
ZKP 数据大小	128 bit

3.2 仿真分析

图 4 显示了平均剩余能量变化的情况。由于本仿真场景中的分发协议 SPIN 几乎固定了分发的路由，所以每轮分发的能耗相差不多。可以发现在 160 轮左右之前四条曲线图近似为直线。与无克隆节点场景（曲线 SPIN）对比，克隆节点越多的网络中曲线的斜率越小，意味着克隆节点越多，导致无法完成数据分发的节点越多，数据分发的可靠性越差。大概在 240 轮以后，由于部分节点能量耗尽而出现了覆盖空洞，曲线的下降速度变的很慢。其中，由于零知识证明的数据相比数据分发中传输的数据大小十分微小，因此即使在 SPIN 方案中应用了单轮零知识证明检测算法，所消耗的能量与不在数据分发中进行节点克隆攻击检测的方案也几乎相等，所以 ZKP-SPIN 与 SPIN 的平均剩余能量曲线几乎完全重合。这在其它的仿真图中也得到了体现，即应用了单轮零知识证明检测方案不会给 SPIN 数据分发协议的性能带来其它损坏。在其它存在 5、10 个克隆节点时的场景中，SPIN 分发协议的分发成功率下降严重，而 ZKP-SPIN 可以在分发过程中即刻进行克隆节点的检测，不会使分发性能受到克隆节点的影响。

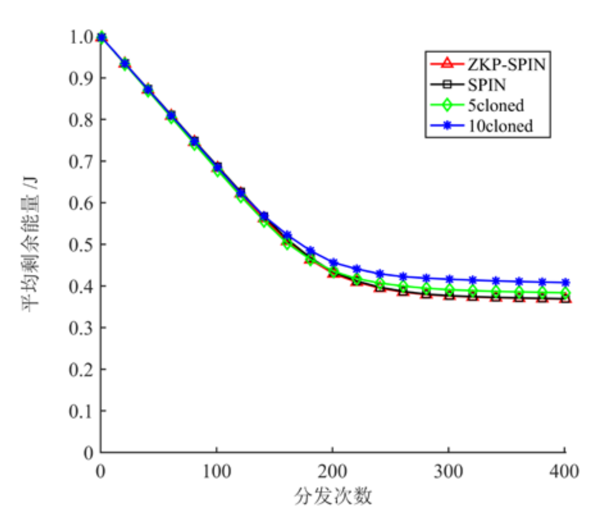


图 4 平均剩余能量随分发次数的变化

图 5 显示了随着数据分发次数的增加，死亡节点数量增加的情况。这里把受到克隆攻击的节点标记为死亡节点。发现四条曲线从分发到第 80 轮左右开始上升，这是因为 Sink 节点周围的节点负担了较大的转发量，能量逐次耗尽成为死亡节点；在数据分发进行到第 240 轮左右时，曲线上升的幅度变小，此时 Sink 的邻居节点几乎能量全部耗尽，形成数据分发的覆盖空洞，所以只有少量几个既是 Sink 的邻居又没有其它存活邻居的节点接收到数据。

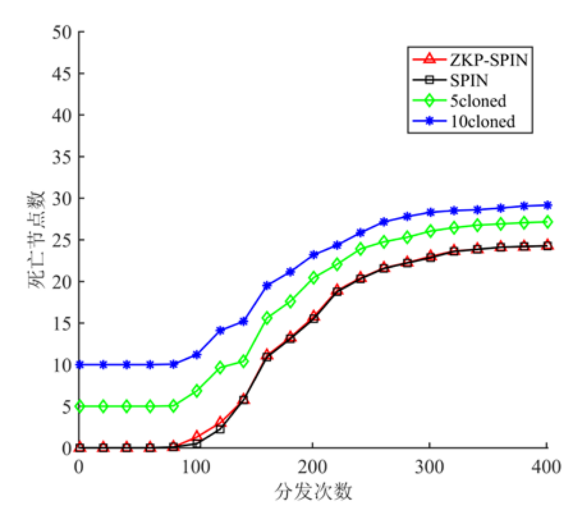


图 5 死亡节点数随分发次数变化

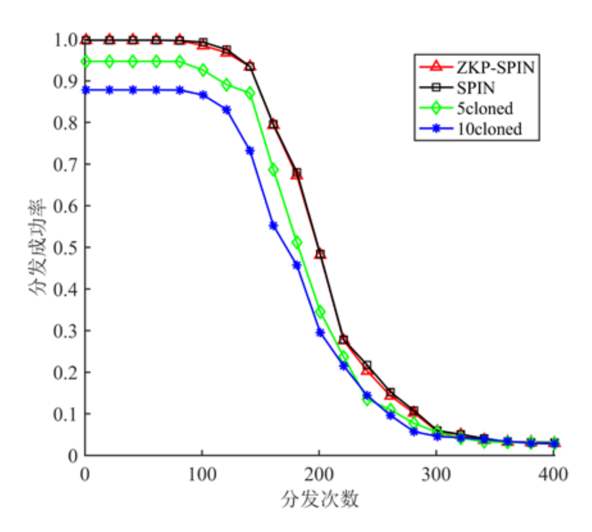


图 6 分发成功率随分发次数的变化

图 6 和图 7 分别显示随着数据分发次数的增加，未能完成数据分发的节点数量增加、数据分发成功率下降的情况。其中未完成数据分发的节点包括 3 种节点：克隆节点、死亡节点和由于出现覆盖空洞而无法与 Sink 节点连通的节点。在无克隆攻击的场景中，随着数据分发不断地进行，能量有限的节点必定会因为能量耗尽而不能完成数据分发。在有克隆节点的场景中，由于仿真中节点克隆攻击是随机发生的，因此克隆节点部署的位置也是随机的。因此当克隆节点被攻击者随机部署在合法节点和 Sink 节点的中间位置时，会导致合法节点把克隆节点作为与 Sink 连接的中间节点，但实际上与 Sink 节点的连接断开，从而无法接收到分发数据。在实际的应用中，智能的攻击者可以有选择地放置克隆节点的位置，使其影响到更多的合法节点，对数据分发可靠性的破坏力更大。尽管由于仿真选择随机部署克隆节点的位置，导致影响到的合法节点数随机，但是仍然可以从图中看出，克隆节点越多的场景对数据分发完成度的破坏性越强。

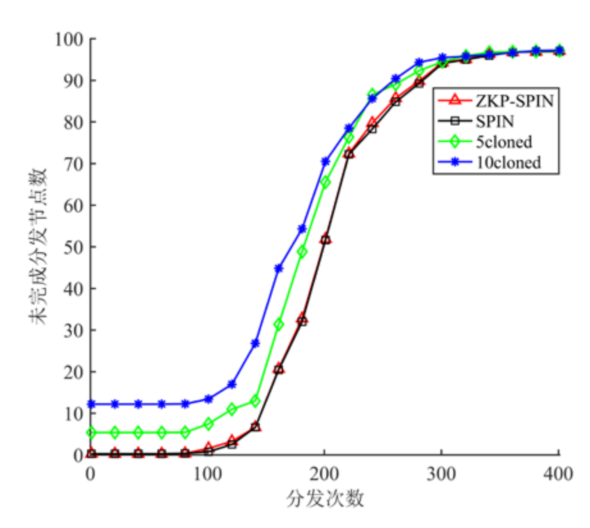


图 7 未完成分发节点数随分发次数的变化

4 结束语

本章节提出了一种基于单轮零知识证明的节点克隆攻击检测方案（SR-ZKP），并将其应用到 SPIN 数据分发协议中，通过该分发模型中的上游节点要求下游节点证明其拥有信息的方案检测是否发生了节点克隆攻击。其中，使用析取-叠加码来生成数字指纹，从而用简单的二进制操作实现复杂的加密；在数字指纹的验证中，应用基于椭圆曲线的单轮零知识证明协议，以确保代表节点真实身份的数字指纹知识不会在证明方和验证方之间的无线信道中传输，保证了数字指纹对 WSNs 中非法第三方的零知识性，同时也避免了中间人攻击和重放攻击。仿真结果表明，该算法不仅实现了对克隆节点的检测，保证了数据分发的可靠性，所产生的能耗也不足以影响数据分发的其它性能。

参考文献：

[1] 孙利民，张书钦，李志等. 无线传感器网络理论及应用[M]. 北京:清华大学出版社, 2018:11-13.
[2] 陈宏滨，陈琪. 能量平衡的无线传感器网络数据采集动态分簇算法[J]. 桂林电子科技大学学报,2020,40(4):286-291.
[3] XU Z R, HU T L, SONG Q S. Bulk data dissemination in low power sensor networks: present and future directions[J]. Sensors, 2017,17(12):156-186.
[4] ZHENG X L, WAN M. A survey on data dissemination in wireless sensor networks[J]. Journal of Computer Science and Technology, 2014,29(3): 470-486
[5] HUANG L J, SETIA S. CORD: Energy-efficient reliable bulk data dissemination in sensor networks[C]// INFOCOM 2008.27th IEEE International Conference on Computer Communications. Piscataway, NJ: IEEE Press, 2008:574-582.
[6] ZHAO Z W, DONG W, BU J J, et al. Exploiting link correlation for core-based dissemination in wireless sensor networks[C]// Eleventh Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). Piscataway, NJ: IEEE Press, 2014:372-380.
[7] ZHU X R, TAO X P, GU T, et al. Target-aware, transmission power-adaptive, and collision-free data dissemination in wireless sensor networks[J]. IEEE Transactions on Wireless Communications, 2015, 14(12):6911-6925.
[8] YU J G, WANG N N, WANG G H, et al. Connected dominating sets in wireless ad hoc and sensor networks-a comprehensive survey[J]. Computer Communications, 2013, 36(2):121-134.
[9] TSENG Y C, NI S, CHEN Y, et al. The broadcast storm problem in a mobile ad hoc network[J]. Wireless Networks, 2002, 8(2-3):153-167.
[10] HASS Z J, HALPERN J Y, LI L. Gossip based ad-hoc routing[C]//IEEE Annual Joint Conference: INFOCOM, IEEE Computer and Communications Societies, Piscataway, NJ: IEEE Press, 2002:1707-1716.
[11] LEVIS P, PATEL N, CULLER D, et al. Trickle: a self-regulating algorithm for code propagation and maintenance in wireless sensor networks[C]// Conference on Symposium on Networked Systems Design & Implementation-volume. Berkeley, CA: USENIX Association, 2004:1-14.
[12] KULIK J, HEINZELMAN W R. Negotiation-based protocols for disseminating information in wireless sensor networks[J]. Wireless Networks,2002, 8(2/3):169-185.
[13] STATHOPOULOS T, HEIDEMANN J, ESTRIN D. A remote code update mechanism for wireless sensor networks[R/OL]. (2003-11-01)[2022-04-24] https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.5.4326
[14] HUI J W, CULLER D. The dynamic behavior of a data dissemination protocol for network programming at scale[C]// SenSys: ACM Conference on Embedded Networked Sensor Systems. New York: ACM, 2004:81-95.
[15] ZHENG X L, WANG J L, DONG W, et al. Bulk data dissemination in wireless sensor networks: analysis, implications and improvement[J]. IEEE Transactions on Computers, 2016,65(5):1428-1439.
[16] AL-RIYAMI A, ZHANG N, KEANE J. An adaptive early node compromise detection scheme for hierarchical WSNs[J]. IEEE Access, 2019, 4:4183-4206.
[17] XING K, LIU F, CHENG X Z, et al. Real-time detection of clone attacks in wireless sensor networks[C]// The 28th International Conference on Distributed Computing Systems. Piscataway, NJ: IEEE Press, 2008:3-10.
[18] RAZA S, WALLGREN L, VOIGT T. SVELTE: Real-time intrusion detection in the Internet of Things[J]. Ad Hoc Networks, 2013, 11(8):2661-2674.
[19] SHANMUGAM A, PARAMASIVAM J. A two-level authentication scheme for clone node detection in smart cities using Internet of things[J]. Computational Intelligence, 2020,36(3):1-21.
[20] LOU Y X, ZHANG Y, LIU S L. Single hop detection of node clone attacks in mobile wireless sensor networks[J]. Procedia Engineering, 2012, 29:2798-2803.
[21] PARNO B, PERRIG A, GLIGOR V. Distributed detection of node replication attacks in sensor networks[C]// 2005 IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE Press, 2005: 49-63.
[22] CORMEN T H, LEISERSON C E, RIVEST R L, et al. Introduction to algorithms[M]. Boston: MIT Press, 2001:89-91.
[23] 孟彦，侯整风，昂东宇，等. 基于椭圆曲线的单轮零知识证明方案[J]. 计算机技术与发展，2007, 17(12):147-150.
[24] BALASUBRAMANIAN R, KOBLITZ N. The improbability that an elliptic curve has subexponential discrete log problem under the menezes-okamoto-vanstone algorithm[J]. Journal of Cryptology, 1998, 11(2):141-145.